Detecting the local indistinguishability of maximally entangled states

Sixia Yu[1, 2] and C.H. Oh[1]

[1] Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, Singapore 117542
[2] Hefei National Laboratory for Physical Sciences at Microscale & Department of Modern Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China

By incorporating the asymmetry of local protocols, i.e., some party has to start with a nontrivial measurement, into an operational method of detecting the local indistinguishability proposed by Horodecki *et al.* [Phys.Rev.Lett. 90 047902 (2003)], we derive a computable criterion to efficiently detect the local indistinguishability of maximally entangled states. Locally indistinguishable sets of d maximally entangled states in a $d \otimes d$ system are systematically constructed for all $d \geq 4$ as an application. Furthermore, by exploiting the fact that local protocols are necessarily separable, we explicitly construct small sets of k locally indistinguishable maximally entangled states with the ratio k/d approaching 3/4. In particular, in a $d \otimes d$ system with even $d \geq 6$, there always exist $d-1$ maximally entangled states that are locally indistinguishable by separable measurements.

Introduction.— Not all properties of a composite system, typically those related to the entanglement, can be accessed locally, i.e., by using only local operations and classical communication (LOCC). This is not surprising as entanglement and nonlocality are intimately related. It is thus striking when a complete set of orthogonal pure product states turns out to be locally indistinguishable [1], i.e., the measurement of some observables with separable eigenstates cannot be implemented locally. This phenomenon of nonlocality without entanglement gives rise to the question as to what properties or global operations can or cannot be measured or implemented locally. The local identification of orthogonal multipartite states, especially the maximally entangled states (MES), provides a perfect tool to explore this boundary.

Orthogonal multipartite states can always be distinguished by global measurements. Even restricted to the local protocols, two orthogonal pure states can always be exactly identified, regardless of the number of parties and whether or not the states are entangled [2]. However, locally indistinguishable sets of three or more orthogonal states do exist, e.g., sets of pure product states[3–5] or MESs [6–11] and even a mixture of them [13]. Due to the complex and elusive structures of LOCC protocols [14], both the demonstration of the local distinguishability, for which one has to build explicit local protocols, and the indistinguishability, for which one has to exclude all possible local protocols, are in general formidable tasks.

Despite our incomplete understanding, there do exist a few properties of of LOCC protocols at our disposal to detect the local indistinguishability. First, LOCC protocols are asymmetric [15–17], i.e., some party has to start with a nontrivial measurement. This seemly innocent property is highly nontrivial, leading to many important results and criteria [18–20]. Second, LOCC protocols cannot increase entanglement, which legitimates entanglement as a resource in various quantum informational tasks. A typical method is the state-identification induced entanglement transformation, the so-called HSSH method [13], which develops from a mixed state version in [6, 21–24]. Third, LOCC protocols belong to some larger family of protocols, such as operations that are separable or having positive partial transpose (PPT), that are relatively well characterized [9, 10, 25, 26].

In this Letter we shall at first combine the asymmetry and HSSH method to detect the local indistinguishability of MESs, called as asymmetric HSSH method here, resulting in a computable criterion. As an application, we present the first complete construction of a locally indistinguishable set of d maximally entangled states in a $d \otimes d$ system for all $d \geq 4$. And then, by exploiting the fact that LOCC protocols are necessarily separable, we are also able to construct so far the smallest set of k maximally entangled states in the case of d being even with the ratio k/d approaching 3/4. After introducing some necessary notations, we shall illustrate the asymmetry and HSSH methods by showing the local indistinguishability of a by far the smallest set of pure product states and a mixture of MESs and a pure product state.

Notations.— Here we shall consider the exact distinguishability of bipartite orthogonal pure states by finite LOCC protocols, i.e., by using local operations plus finite rounds of classical communication we would like to identify a state from a given set without any error. A set of mutually orthogonal pure states $\{|\psi_r\rangle\}$ is distinguished by a measurement $\{M_r\}$ if

$$\langle\psi_s|M_r|\psi_s\rangle = \delta_{rs}. \tag{1}$$

If the measurement can be implemented by finite LOCC protocols or each M_r is separable, then the set $\{|\psi_r\rangle\}$ is locally distinguishable or distinguishable by separable measurement, respectively.

A bipartite system of two qudits, labeled with A and B, is simply denoted by $d \otimes d$. For each qudit, we denote by $\{|n\rangle\}$ with $n \in \mathbb{Z}_d := \{0, 1, \ldots, d-1\}$ its computational basis, by I the identity operator, and by

$$X = \sum_{n\in\mathbb{Z}_d} |n+1\rangle\langle n|, \quad Z = \sum_{n\in\mathbb{Z}_d} \omega^n |n\rangle\langle n|, \tag{2}$$

its bit and phase flip operators, respectively, satisfying a Weyl-type commutation relation $ZX = \omega XZ$ with $\omega = e^{i2\pi/d}$. These operators are subscripted by the dimension they act on when necessary. In the case of qubit $d = 2$ we shall denote by $\{\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ the identity and three Pauli operators. In a $d \otimes d$ system, let

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{n\in\mathbb{Z}_d} |n\rangle \otimes |n\rangle \tag{3}$$

denote the standard maximally entangled state (MES). Each MES can be written as $|\psi_U\rangle = U \otimes I|\Phi\rangle$ for some unitary U and we shall represent a set of MESs $\{|\psi_U\rangle\}$ also by the set $\{U\}$ of the corresponding unitaries. For convenience we shall denote by $\psi_U = |\psi_U\rangle\langle\psi_U|$ the density matrix of a pure state $|\psi_U\rangle$. For two orthogonal MESs represented by U and V it holds $\mathrm{Tr}(UV^\dagger) = 0$. The set of MESs $\{U_{st} = X^s Z^t\}$ is also referred to as MESs in canonical form or generalized Bell states.

Indistinguishability by asymmetry.— Local protocols for discrimination are asymmetric: some party has to start with a *nontrivial* and *non-disturbing* measurement, i.e., not all outcome M_r is proportional to identity and after which the orthogonality relations are preserved, making further discrimination possible. The method by asymmetry first appeared in [15] and was elaborated in [16, 17] and further developed in [19, 20]. Our first result is by far the smallest set of locally indistinguishable pure product states that demonstrates nonlocality without entanglement.

Theorem 1 *In a $d \otimes d$ system with $d \geq 3$ the following $2d-1$ orthogonal pure product states are locally indistinguishable:*

$$\{|n\rangle \otimes |\delta_n\rangle\}_{n=1}^{d-1} \cup \{|\delta_n\rangle \otimes |n_+\rangle\}_{n=1}^{d-1} \cup \{|\theta_0\rangle \otimes |\theta_0\rangle\}, \tag{4}$$

where $|\theta_0\rangle \propto \sum_j |j\rangle$ and $|\delta_n\rangle \propto |n\rangle - |0\rangle$ and $n_+ = n+1$ for $1 \leq n \leq d-2$ while $n_+ = 1$ for $n = d-1$.

Proof We denote by $\{|\varphi_r\rangle\}$ those $2d-1$ pure product states and they are mutually orthogonal since $n_+ \neq 0, n$ and $|\delta_n\rangle$ is orthogonal to $|\theta_0\rangle$. Suppose that this set is locally distinguishable then someone, say, Alice, has to start with a nontrivial and nondisturbing measurement $\{M_A\}$, i.e., not all M_A are proportional to identity and the post measurement states $\{\sqrt{M_A} \otimes I_B|\varphi_r\rangle\}$ should also be mutually orthogonal. As a result we have $\langle n|M_A|n'\rangle\langle\delta_n|\delta_{n'}\rangle = 0$ for all nonzero $n \neq n'$, from which it follows that $\langle n|M_A|n'\rangle = 0$, and $\langle n'|M_A|\delta_n\rangle\langle\delta_{n'}|n_+\rangle = 0$, which in turn leads to $\langle n_+|M_A|0\rangle = 0$ for all nonzero n since $\langle\delta_{n'}|n\rangle = 0$ unless $n = n'$. Thus all non diagonal elements of M_A have to vanish. From the orthogonality $\langle\theta_0|M_A|\delta_k\rangle\langle\theta_0|n_+\rangle = 0$ it follows that $\langle n|M_A|n\rangle = \langle 0|M_A|0\rangle$ for all $n \neq 0$, i.e., M_A is proportional to identify, meaning that Alice cannot start with a nontrivial measurement. For the same reason Bob cannot start with a nontrivial measurement either. Therefore the set $\{|\varphi_r\rangle\}$ is locally indistinguishable. □

After its discovery, nonlocality without entanglement is usually demonstrated by unextendible product basis (UPB) [3, 4], a set of mutually orthogonal pure product states that spans a subspace whose complementary subspace contains no pure product state. Despite of being a natural generalization of a UPB in a 3×3 system to higher dimensions, our set is extendible for all $d \geq 4$. The following $d-1$ mutually orthogonal pure product states $(|0\rangle + |n\rangle - 2|(n_+)_+\rangle) \otimes |n_+\rangle$ for $n = 1, 2, \ldots d-1$ are orthogonal to all the pure product states in Eq.(4). In the case of odd d our set is of the same size as the minimal UPB while in the case of even d our set is one state smaller than the smallest UPB, which contains at least $2d$ states [27]. Although the smallest number of locally indistinguishable pure product states remains unknown, we conjecture that our sets are minimal, i.e., any set of no more than $2(d-1)$ product states is locally distinguishable, which is true for $d = 3$ since any 4 product states are shown to be locally distinguishable [4].

HSSH method.— Local protocols cannot increase entanglement and local discrimination can be part of LOCC protocols, e.g., inducing a local entanglement transfer between some specific pure states. The HSSH method [13] exploits this fact to detect the local indistinguishability when such a local state transformation is impossible, which is illustrated by our second result.

Theorem 2 *In a $d \otimes d$ system with $d \geq 3$ the following $k = [d/2] + 1$ maximally entangled states*

$$\{I, Z, Z^2, \ldots, Z^{[\frac{d}{2}]}\} \tag{5}$$

together with one pure product state $|1\rangle \otimes |0\rangle$, are locally indistinguishable.

Proof We denote by $\Gamma = \{|\phi_r\rangle\}_{r=0}^{k}$ those $k+1$ states given above, with the last one being the pure product state. By introducing two auxiliary qudits C and D we build the so-called detector state, as the first step of HSSH method, i.e., a 4-qudit pure state,

$$\begin{aligned} |\Psi_\Gamma\rangle_{AC:BD} &= \sum_{r=0}^{k-1} \sqrt{p_r}|\phi_r\rangle_{AB} \otimes |\psi_r\rangle_{CD} \\ &:= dT_{AC} \otimes I_{BD}|\Phi\rangle_{AC:BD}, \end{aligned} \tag{6}$$

where $|\Phi\rangle_{AC:BD} = |\Phi\rangle_{AB} \otimes |\Phi\rangle_{CD}$, $|\psi_r\rangle = |\phi_r^*\rangle$ for $r = 0, 1, \ldots, k-1$ and $|\psi_k\rangle = |\psi_X\rangle = X \otimes I|\Phi\rangle$, and

$$T_{AC} = \frac{1}{d}\sum_{r=0}^{k-1} \sqrt{p_r} Z^r \otimes Z^{-r} + \sqrt{\frac{p_k}{d}}|1\rangle\langle 0| \otimes X \tag{7}$$

with $p_k = b$ and $p_r = a$ for $0 \leq r \leq k-1$ with $ka + b = 1$ and $b = d/(4k-d) < 1$, recalling that $k > d/2$. Every local protocol successfully discriminating Γ, followed by a suitable local unitary transformation, presents a local protocol of state transfer $\Psi_\Gamma \to \Phi$ in the $AC : BD$ cut.

According to [28–30] the local state transfer $\Psi_\Gamma \to \Phi$ is possible if and only if $\lambda_1(\Psi_\Gamma) \leq 1/d$ where $\lambda_1(\Psi_\Gamma)$

denotes the largest Schmidt coefficient of $|\Psi_\Gamma\rangle_{AC:BD}$, i.e., the largest eigenvalue of $M_{AC} = T_{AC}T_{AC}^\dagger$. However, in the 2-dimensional subspace spanned by $\{|0,0\rangle, |1,1\rangle\}_{AC}$ the matrix M_{AC} has matrix elements

$$\tilde{M}_{AC} = \frac{1}{d^2}\begin{pmatrix} ak^2 & k\sqrt{dab} \\ k\sqrt{dab} & ak^2 + db \end{pmatrix} \tag{8}$$

from which it follows

$$\lambda_1(\Psi_\Gamma) \geq \lambda_1(\tilde{M}_{AC}) = \frac{1}{d} + \frac{(2k-d)^2}{d^2(4k-d)} > \frac{1}{d},$$

meaning that the local entanglement transfer $\Psi_\Gamma \to \Phi$, so that the local discrimination of Γ, is impossible. □

We note that, first, if the pure product state is replaced by a MES, e.g., $Z^\dagger$, then the set becomes locally distinguishable, demonstrating a counterintuitive phenomenon of more nonlocality with less entanglement [13]. Second, as noted in [25], the HSSH method alone cannot detect the local indistinguishability of d MESs in a $d\otimes d$ system. Actually, for any set Γ of d MESs the following 4-partite pure state, which is the most general detector,

$$|\Psi\rangle_{AC:BD} = \sum_{L\in\Gamma} \sqrt{p_L}|\psi_L\rangle_{AB} \otimes |\psi_{L'}\rangle_{CD}, \tag{9}$$

where $\{|\psi_{L'}\rangle\}$ are MESs in some auxiliary systems C and D of dimension d', can always be transformed into $|\Phi\rangle_{CD}$ by LOCC. This is because the largest singular value of $T_{AC} = \sum_L \sqrt{p_L} L \otimes L'/\sqrt{dd'}$ is at most $1/\sqrt{d'}$, i.e., we always have $\lambda_1(\Psi) \leq 1/d'$, which ensures a local transfer of Ψ into a MES [28, 29].

Asymmetric HSSH method.— We shall consider the local indistinguishability of a set of $k \leq d$ MESs in a $d\otimes d$ system, since any number $k > d$ of MESs cannot be locally distinguished [7], even by PPT measurements [8, 9]. It turns out that any triplet of MESs in a $3\otimes 3$ system is locally distinguishable [7] and in a $4\otimes 4$ there is a PPT indistinguishable quadruple of MESs [8], which was generalized to the case of d being a power of 2 [9], for which small sets of $k < d$ indistinguishable MESs were also constructed [10]. An almost comprehensive construction of d MESs in a $d\otimes d$ was provided [11] except for $d = 5, 11$ [12]. Because of its relative small size i.e., $k \leq d$, there are not enough orthogonality conditions to exclude a nontrivial measurement so that the asymmetry method alone does not work either. However, a combination of those two methods above turns out to be extremely effective.

Theorem 3 *In a $d\otimes d$ system with $d \geq 4$ the following set of d maximally entangled states*

$$\Gamma_d = \{I, Z, Z^2, \ldots, Z^{d-3}, X^{[\frac{d}{2}]}, X^{\dagger[\frac{d}{2}]}Z^\dagger\} \tag{10}$$

is locally indistinguishable.

Proof Suppose that the states are locally distinguishable and someone, say Alice, has to start with a nontrivial measurement $\{M\}$, i.e., there is at least one M that is *not* proportional to the identity. After the A-measurement the set $\{|\psi_L\rangle \mid L \in \Gamma_d\}$ is transformed into

$$\{|\phi_L\rangle = \sqrt{dM'} \otimes I|\psi_L\rangle \mid L \in \Gamma_d\},\ M' = M/\mathrm{Tr}M \tag{11}$$

accordingly, which must also be mutually orthogonal in order to be distinguishable by further local protocols. By introducing two auxiliary qudits C and D we take the following 4-qudit pure state as the detector state

$$\begin{aligned} |\Psi_{\Gamma_d}\rangle_{AC:BD} &:= \frac{1}{\sqrt{d}}\sum_{L\in\Gamma_d} |\phi_L\rangle_{AB} \otimes |\psi_{L^*}\rangle_{CD} \\ &:= dT_{AC} \otimes I_{BD}|\Phi\rangle_{AC:BD}, \end{aligned} \tag{12}$$

where $T_{AC} = \sum_{L\in\Gamma_d}(\sqrt{M'}L) \otimes L^*/d$. The local entanglement transfer $\Psi_{\Gamma_d} \to \Phi$ is possible if and only if the largest Schmidt coefficient $\lambda_1(\Psi_{\Gamma_d}) \leq 1/d$.

Since $\lambda_1(\Psi_{\Gamma_d})$ is given by the largest eigenvalue of $M_{AC} = T_{AC}T_{AC}^\dagger$, we have a lower bound

$$\lambda_1(\Psi_{\Gamma_d}) \ \geq\ \frac{\langle\varphi|M_{AC}|\varphi\rangle}{\langle\varphi|\varphi\rangle} = \frac{1}{d} + \frac{\mathrm{Tr}(M_{\Gamma_d} - I)^2}{d^2} \tag{13}$$

where $|\varphi\rangle = \sqrt{M} \otimes I|\Phi\rangle$ and $M_{\Gamma_d} = \sum_{L\in\Gamma_d} L^\dagger M' L$. If we can prove $M_{\Gamma_d} \neq I$ then we have $\lambda_1(\Psi_{\Gamma_d}) > 1/d$ so that the local transfer, as well as the local discrimination, is impossible. Here is exactly where the asymmetry enters into the play: we have only to show that for any nontrivial and non-disturbing M it holds $M_{\Gamma_d} \neq I$, i.e., there exists $(s,t) \neq (0,0)$ with $s,t \in \mathbb{Z}_d$ such that $0 \neq \mathrm{Tr}(M_\Gamma U_{st}) = M_{st}\gamma_{st}/\mathrm{Tr}M$ where

$$\begin{aligned} \gamma_{st} &:= \frac{1}{d}\sum_{L\in\Gamma_d} \mathrm{Tr}(U_{st}^\dagger L U_{st} L^\dagger) \\ &= d\delta_{s0} - \omega^{-2s} - \omega^{-s} + \omega^{-[\frac{d}{2}]t} + \omega^{[\frac{d}{2}]t-s} \end{aligned} \tag{14}$$

and $M_{st} = \mathrm{Tr}(MU_{st})$, recalling that $U_{st} = X^sZ^t$. Since M is nontrivial, i.e., there exists $(s,t) \neq (0,0)$ such that $M_{st} \neq 0$, it suffices to show that $\gamma_{st} \neq 0$ or $\gamma_{st} = 0$ infers $M_{st} = 0$ for all $s,t \in \mathbb{Z}_d$. In the case of odd d we have $\gamma_{0t} \neq 0$ since $d \geq 5$ and

$$\gamma_{st} = 2\omega^{[\frac{d}{2}]s}\left(\cos\frac{2[\frac{d}{2}](s+t)}{d}\pi - \omega^{-s}\cos\frac{2[\frac{d}{2}]s}{d}\pi\right) \neq 0$$

for all $t \in \mathbb{Z}_d$ if $s \neq 0$ since ω^s is not real. As a result we have $\gamma_{st} \neq 0$ for all $s,t \in \mathbb{Z}_d$. In the case of even d

$$\gamma_{st} = d\delta_{s0} + \big((-1)^t - \omega^{-s}\big)(1 + \omega^{-s})$$

since $\omega^{d/2} = -1$. If $d = 4$ then $\gamma_{st} = 0$ if and only if $(s,t) \in \{(0,1), (0,3), (2,t)\}$ and in these cases we have $M_{st} = 0$ due to the fact that $\mathrm{Tr}(ML'L^\dagger) = 0$ for different $L, L' \in \Gamma_d$ as a result of $\{|\phi_L\rangle\}$ being mutually orthogonal, e.g., $\mathrm{Tr}(MZ^{\pm1}) = 0$. If $d \geq 6$ then $\gamma_{st} = 0$ if and only if $s = d/2$ with t being arbitrary. From the orthogonality relationship of $\{|\phi_L\rangle\}$ it is straightforward to check that $\mathrm{Tr}(MX^{d/2}Z^t)=0$ for all $t\in\mathbb{Z}_d$, taking into account that $X^{d/2}$ is Hermitian. □

Some remarks are in order. First, the proof above actually leads to a computable sufficient condition to detect the local indistinguishability of d MESs in a $d\otimes d$ system. We define a Weyl basis $\mathcal{W}$ to be an orthogonal unitary operator basis in which $U_1U_2\propto U_2U_1$ for each pair of $U_{1,2}\in\mathcal{W}$. The basis $\{U_{st}=X^sZ^t\}$ for a general qudit is one example. In the case of each subsystem bing a composite of multi qubits, all the multi qubit Pauli operators provide another example.

Lemma *In a $d\otimes d$ system, a subset of a Weyl basis, i.e., $\mathcal{L}\subset\mathcal{W}$, defines a locally indistinguishable set of d maximally entangled states if $|\mathcal{L}|=d$ and*

$$K(\mathcal{L})\subseteq\Delta(\mathcal{L}) \tag{15}$$

where $K(\mathcal{L})=\{U\in\mathcal{W}|\gamma_U=0\}$ denotes the kernel set and $\Delta(\mathcal{L}):=\{L_1L_2^\dagger\mid L_1,L_2\in\mathcal{L}\}$ denotes the pairwise difference set with

$$\gamma_U=\frac{1}{d}\sum_{L\in\mathcal{L}}\mathrm{Tr}(LUL^\dagger U^\dagger). \tag{16}$$

The proof of Lemma can proceed in exactly the same manner as the proof of Theorem 1 all the way to Eq(13), with Γ_d replaced by $\mathcal{L}$. The condition Eq.(15) ensures that a nontrivial M leads to the existence of $U\in\mathcal{W}$ with $U\neq I$ such that $M_U\gamma_U\neq 0$ which makes $M_{\mathcal{L}}=\sum_{L\in\mathcal{L}}L^\dagger ML/\mathrm{Tr}M\neq I$ so that $\lambda_1(\Psi_{\mathcal{L}})>1/d$. Here, since $\mathcal{W}$ is a basis, we have expansion $M=\sum_{U\in\mathcal{W}}M_UU^\dagger/d$ with $M_U=\mathrm{Tr}(MU)$. For an example, in the case of even $d\geq 4$ the set

$$\Gamma_e=\{I,Z,Z^2,\ldots,Z^{d-2},X^{d/2}\} \tag{17}$$

can be shown to be locally indistinguishable since we have $K(\Gamma_e)=\{X^{dt/2}Z^t\mid t\neq 0\}$ while $\Delta(\Gamma_e)=\{X^{ds/2}Z^t\mid(s,t)\neq(0,0)\}$. The indistinguishability of Γ_e in the case of $d=4,6$ was conjectured [6] and checked numerically [9]. The local indistinguishability of five MESs $\{I,XZ,XZ^2,X^3Z,X^3Z^2\}$ in a $5\otimes 5$ system, which is verified numerically also in [9], can now be analytically proved since K is an empty set. A quadruple $\{I,XZ,XZ^3,X^2Z^3\}$ is shown to be indistinguishable by one-way LOCC protocols and conjectured to be locally indistinguishable [31], which turns out to be true according to our criterion since we have $K=\{Z^2\}\subset\Delta$.

For the last example we consider a $4\otimes 4$ system with each subsystem regarded as a composite system of two qubits. The identity and 15 Pauli operators of a 2-qubit system form a Weyl basis. The first example of LOCC indistinguishable set of d MESs in a $d\otimes d$ system, i.e., a quadruple $\mathcal{L}_4=\{\mathcal{I}_1\mathcal{I}_2,\mathcal{X}_1\mathcal{X}_2,\mathcal{Y}_1\mathcal{X}_2,\mathcal{Z}_1\mathcal{X}_2\}$ of MESs [8], is a subset of this Weyl basis. It is straightforward to check that $K(\mathcal{L}_4)=\Delta(\mathcal{L}_4)=\{\mathcal{X},\mathcal{Y},\mathcal{Z}\}\otimes\{\mathcal{I},\mathcal{X}\}$ and the local indistinguishability of $\mathcal{L}_4$ follows immediately from our Lemma.

Second, unlike previous constructions of indistinguishable sets of MESs where the properties of PPT or separable measurements are employed, our construction deals with LOCC protocols directly. This makes it easier for a complete construction of d MES in a $d\otimes d$ for all dimensions d on the one hand and on the other hand we cannot exclude the possibility of being distinguished by some PPT or separable measurements, or even asymptotic LOCC protocols.

Small set of locally indistinguishable MESs.— Every LOCC protocol is separable so that it has positive partial transpose. This property has been used to construct small sets of $k<d$ locally indistinguishable MESs in a system $d\otimes d$ with d being a power of 2 [10], which is significantly improved by our last result:

Theorem 4 *In a $2d\otimes 2d$ system with $d\geq 2$ there exist $k_\sigma=2d-q+\sigma$ maximally entangled states that are indistinguishable by separable measurements, where q is the largest proper divisor of d and $\sigma=1$ if d is even and 0 if d is odd.*

Proof For any $d\geq 2$ with q being its largest proper divisor, i.e., $q\neq d$ being the largest integer that divides d, there is a prime $p\geq 2$ such that $d=pq$ and $q\geq p$ if $q\neq 1$. Each subsystem can be regarded as a composite system of a qubit and two qudits with p and q levels. We claim that the following set of $k_\sigma=2d-q+\sigma$ MESs is indistinguishable by separable measurements:

$$\Xi_{2d}=\{Z_q^n\otimes L_V\mid n\in\mathbb{Z}_q,V\in\mathcal{L}_p^\sigma\}, \tag{18}$$

where $L_V=|0\rangle\langle 1|\otimes V-|1\rangle\langle 0|\otimes V^T$ and

$$\mathcal{L}_p^\sigma=\{Z_p^a\}_{a=0}^{p-2+\sigma}\cup\{X_pZ_p^a\}_{a\in\mathbb{Z}_p}, \tag{19}$$

because of the following contradiction

$$\begin{aligned}0&=k_\sigma-\sum_{U\in\Xi_{2d}}\mathrm{Tr}(M_U\psi_U)\\&=k_\sigma-\mathrm{Tr}H_{2d}+\sum_{U\in\Xi_{2d}}\mathrm{Tr}M_U(H_{2d}-\psi_U)\\&\geq\sum_{U=Z_q^n\otimes L_V\in\Xi_{2d}}\mathrm{Tr}M_U(P_q\otimes H_{L_V})+\sigma>0,\end{aligned} \tag{20}$$

where we have denoted $H_{2d}=P_q\otimes A_{2p}$ and $H_{L_V}=A_{2p}-\psi_{L_V}$ with

$$P_q=\sum_{n\in\mathbb{Z}_q}|n,n\rangle\langle n,n|,\quad A_{2p}=\frac{I_{2p}\otimes I_{2p}-V_{2p}}{2p} \tag{21}$$

and V_{2p} being the swap operator on the $2p\otimes 2p$ system.

Suppose that the set Ξ_{2d} can be distinguished by some separable measurement $\{M_U\}_{U\in\Xi_{2d}}$, i.e., $\mathrm{Tr}(M_U\psi_{U'})=\delta_{UU'}$ for arbitrary $U,U'\in\Xi_{2d}$, from which the first equality in Eq.(20) follows immediately by noting $|\Xi_{2d}|=k_\sigma$. The second equality is due to the completeness of the measurement. The first inequality holds because $\mathrm{Tr}H_{2d}=2d-q$ and $P_q=\sum_{n\in\mathbb{Z}_q}\psi_{Z_q^n}$ so that $\psi_U=$

d	k_{min}
4 or $p \geq 5$ (prime)	d
$2p$ ($p \geq 3$ prime)	$d-1$
$4m$ ($m \geq 2$)	$\frac{3}{4}d+1$
$6m$ ($m \geq 1$ odd)	$\frac{5}{6}d$
$2pq$ ($p \geq 5$ prime, $q \geq p$ odd)	$\frac{2p-1}{2p}d$

TABLE I: The smallest size k_{min} of the locally indistinguishable sets of MESs in all possible local dimension d as constructed form Theorem 3 and 4.

$\psi_{Z_q^n} \otimes \psi_{L_V} \leq P_q \otimes \psi_{L_V}$. The last inequality holds because we have, firstly,

$$\mathrm{Tr} M(P_q \otimes H_{L_V}) \geq 0, \ \forall \ L_V \in \mathcal{L}_p^\sigma, \tag{22}$$

for any separable $M \geq 0$ and, which immediately proves the theorem in the case of even d, and secondly,

$$\mathrm{Tr} M_{I_q \otimes L_I}(P_q \otimes H_{L_I}) > 0 \tag{23}$$

in the case of odd d, both of which will be proved in Appendix. Actually H_{L_V}, as well as $P_d \otimes H_{L_V}$, defines an entanglement detecting positive map [32, 33] which has been used in [26] to detect indistinguishability by separable measurements in the case of $p = 2$. □

The minimal size of a locally indistinguishable sets of MESs inferred form Theorem 3 and 4 is summarized in Table I. Notably, in a $4m \otimes 4m$ system with $m \geq 1$ there is a set of $k = 3m + 1$ locally indistinguishable MESs. Specially, in a $8m \otimes 8m$ system with $m \geq 1$ there exist $6m+1$, instead of $7m+1$ in [10], locally indistinguishable MESs. In the limit of large d the ratio k/d approaches 3/4. As another consequence, in the case of even $d \geq 6$ we have $q - \sigma \geq 1$ so that there always exists a set of $d - 1$ MESs that is locally indistinguishable.

Conclusions and discussions.— We have exploited various properties of LOCC protocols to detect the exact local distinguishability of maximally entangled states. A computable criterion is derived by which many previously conjectured or only numerically checked indistinguishable sets of MESs are confirmed. A complete construction of d MESs in a $d \otimes d$ system is provided for all $d \geq 4$ for the first time as well as small sets of locally indistinguishable MESs comparing to the local dimension. Our method may also help in investigating the distinguishability by asymptotic LOCC protocols or unambiguous discrimination. Detection of the indistinguishability is only the first step, showing that there is nonlocality somewhere. The next step is to quantify the necessary nonlocal resource, such as entanglement, to complete the task of local discrimination.

Acknowledgement.— This work is funded by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and the National Research Foundation, Singapore (Grant No. WBS: R-710-000-008-271).

[1] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin and W.K. Wootters, *Quantum nonlocality without entanglement*, Phys. Rev. A **59**, 1070 (1999).

[2] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, *Local distinguishability of multipartite orthogonal quantum states*, Phys. Rev. Lett. **85**, 4972 (2000).

[3] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, *Unextendible product bases and bound entanglement*, Phys. Rev. Lett. **82**, 5385 (1999).

[4] D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, *Unextendible product bases, uncompleteable product bases and bound entanglement*, Commun. Math. Phys. **238**, 379 (2003).

[5] Y. Feng and Y. Shi, *Characterizing locally indistinguishable orthogonal product states*, IEEE. Tran. on Inf. **55**, 2799 (2009).

[6] S. Ghosh S, G. Kar, A. Roy, and D. Sarkar, *Distinguishability of maximally entangled states*, Phys. Rev. A **70** 022304 (2004).

[7] M. Nathanson, *Distinguishing bipartite orthogonal states by LOCC: best and worst cases*, J. Math. Phys. **46** 062103 (2005).

[8] N. Yu, R. Duan, and M. Ying, *Four Locally indistinguishable ququad-ququad orthogonal maximally entangled states*, Phys. Rev. Lett. **109**, 020506 (2012).

[9] A. Cosentino, *Positive-paritial-transpose indistinguishable states via semidefinite programming*, Phys. Rev. A **87**, 012321 (2013).

[10] A. Cosentino, and V. Russo, *Small sets of locally indistinguishable orthogonal maximally entangled states*, Quant. Inf. & Compt. **14** 1098 (2014).

[11] M.-S. Li, Y.-L. Wang, S.-M. Fei, and Z.-J. Zheng, *d PPT-indistinguishable maximally entangled states in* $\mathbb{C}^d \otimes \mathbb{C}^d$ arXiv:1411.6702 (2014).

[12] In [11] the construction for $d = 5$ refers to the numerical result in [9], which is confirmed here, while in the construction for $d = 11$ some of those 12 states, namely V_{3+i} and V_{9+i}, are not orthogonal.

[13] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, *Local distinguishability: more nonlocality with less entanglement*, Phys. Rev. Lett. **90** 047902 (2003).

[14] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, A. Winter*Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask)*, Commun. Math. Phys. **328**, 303 (2014).

[15] B. Groisman and L. Vaidman, *Nonlocal observables with product-state basis*, J. Phys. A: Math. Gen. **34**, 6881 (2001).

[16] J. Walgate and L. Hardy, *Nonlocality, asymmetry and distinguishing bipartite states*, Phys. Rev. Lett. **89** 147901 (2002).

[17] J. Niset and N.J. Cerf, *Multipartite nonlocality without entanglement in many dimensions*, Phys. Rev. A **74**, 052103 (2006).

[18] P.-X. Chen and C.-Z. Li, *Orthogonality and distinguishability: criterion for local distinguishability of arbitrary orthogonal states*, Phys. Rev. A **68** 062107 (2003).

[19] M.-Y. Ye, W. Jian, P.-X. Chen, Y.-S. Zhang, Z.-W. Zhou, and G.-C. Guo, *Local distinguishability of orthogonal quantum states and generators of SU(N)*, Phys. Rev.

A **76**, 032329 (2007).

[20] S.M. Cohen, *Local distinguishability with preservation of entanglement*, Phys. Rev. A **75**, 052313 (2007).

[21] S. Ghosh, G. Kar, A. Roy, A. Sen (De), and U. Sen, *Distinguishability of Bell states*, Phys. Rev. Lett. **87**, 277902 (2001).

[22] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen(De), and U. Sen, *Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement*, Phys. Rev. A **65**, 062307 (2002).

[23] D. Yang and Y.-X. Chen, *Distinguishing maximally entangled states locally*, arXiv: quant-ph/0311100v1.

[24] H. Fan *Distinguishability and indistinguishability by local operations and classical communication*, Phys. Rev. Lett. **92** 177905 (2004).

[25] N. Yu, R. Duan, and M. Ying, *Distinguishability of quantum states by positive operator-valued measures with positive partial transpose*, IEEE Trans. Inf. Theory **60**, 2069 (2014).

[26] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu. *Limitations on separable measurements by convex optimization*, arXiv:1408.6981 (2014).

[27] J. Chen and N. Johnston, *The minimum size of unextendible product bases in the bipartite case (and some multipartite cases)*, Commun. Math. Phys. **333**, 351 (2015).

[28] H.-K. Lo and S. Popescu, *Concentrating entanglement by local actions: Beyond mean values*, Phys. Rev. A **63**, 022301 (2001).

[29] M.A. Nielson, *Conditions for a class of entanglement transformations*, Phys. Rev. Lett. **83**, 436 (1999).

[30] G. Vidal, *Entanglement of pure states for a single copy*, Phys. Rev. Lett. **83**, 1046 (1999).

[31] S. Bandyopadhyay, S. Ghosh, and G. Kar, *LOCC distinguishability of unilaterally transformable quantum states*, New J. Phys. **13**, 123013 (2011).

[32] H. Breuer, *Optimal entanglement criterion for mixed quantum states*, Phys. Rev. Lett. **97**, 080501 (2006).

[33] W. Hall, *A new criterion for indecomposability of positive maps*, J. of Phys. A: Math. & Gen., **39**, 14119 (2006).

Appendix: Proof of Eq.(22) and Eq.(23).— Since L_V is antisymmetric, i.e., $L_V^T = -L_V$ for all $V \in \mathcal{L}_p^\sigma$, and $|y^*\rangle\langle y|$ is symmetric for an arbitrary state $|y\rangle$ in the $2p$ system, we have $\langle y|L_V|y^*\rangle = 0$, from which it follows

$$2p\mathrm{Tr}(x\otimes y)H_{L_V} = 1 - |\langle x|y\rangle|^2 - |\langle x|L_V|y^*\rangle|^2 \geq 0 \quad (24)$$

for arbitrary two normalized pure states $|x\rangle$ and $|y\rangle$ in the $2p$ system. As a result, for an arbitrary pure state $|z\rangle_A = \sum_n |n\rangle \otimes |x_n\rangle$ and $|w\rangle_B = \sum_n |n\rangle \otimes |y_n\rangle$ on each subsystem A and B it holds

$$\mathrm{Tr}(z_A \otimes w_B)(P_q \otimes H_{L_V}) = \sum_{n\in\mathbb{Z}_q} \mathrm{Tr}(x_n \otimes y_n) H_{L_V} \geq 0 \quad (25)$$

since $\mathrm{Tr}_q(z_A\otimes w_B)P_q = \sum_n x_n \otimes y_n$, with the trace taken over the q systems from both A and B. As a result we obtain Eq.(22) immediately by noting that any separable $M \geq 0$ is a convex combination of pure product states.

Now we suppose $d = pq$ is odd so that $p \geq 3$. If the inequality in Eq.(23) were not true then from Eq.(22) it would follow $\mathrm{Tr}M_{U_0}(P_q \otimes H_{L_I}) = 0$ for $U_0 = I_q \otimes L_I$, which would lead to, as will be shown below, the existence of a non-zero operator $R \geq 0$ of the qudit with p levels such that

i. R is of rank at most two;

ii. $\mathrm{Tr}(RV) = 0$ for all $V \in \mathcal{L}_p^0$ with $V \neq I$.

In fact, since M_{U_0} is separable, we have $M_{U_0} = \sum_j z_j \otimes w_j$ for some pure states $|z_j\rangle_A = \sum_n |n\rangle \otimes |x_{j,n}\rangle$ and $|w_j\rangle_B = \sum_n |n\rangle \otimes |y_{j,n}\rangle$. From $\mathrm{Tr}M_{U_0}(P_q \otimes H_{L_I}) = 0$ it would follow that both Eq.(24) and Eq.(25) become now equalities, meaning that $|x_{j,n}\rangle$ should live in the subspace spanned by orthogonal states $\{|y_{j,n}\rangle, L_I|y^*_{j,n}\rangle\}$, i.e., $|x_{j,n}\rangle = c_{j,n}|y_{j,n}\rangle + e_{j,n}L_I|y^*_{j,n}\rangle$ with $c_{j,n}, e_{j,n}$ being some complex numbers, for arbitrary j, n. From the distinguishability conditions $\mathrm{Tr}(M_{U_0}\psi_U) = \delta_{UU_0}$ for all $U = Z_q^l \otimes L_V \in \Xi_{2d}$ we obtain

$$\sum_j \left| \sum\nolimits_{n\in\mathbb{Z}_q} \omega_q^{ln} e^*_{j,n} \mathrm{Tr}(L_I^\dagger L_V y^T_{j,n}) \right|^2 = \delta_{VI}\delta_{l0}, \quad (26)$$

recalling that $y^T_{j,n} = |y^*_{j,n}\rangle\langle y^*_{j,n}|$. From the condition Eq.(26) in the case of $V = I$, it follows that $e^*_{j,n}\mathrm{Tr}y^T_{j,n}$ is independent of n and is nonzero for at least one j. For such a j, from the condition Eq.(26) in the case of $V \neq I$ we obtain, taking into account $e_{j,n} \neq 0$,

$$0 = \mathrm{Tr}(L_I^\dagger L_V y^T_{j,n}) = \mathrm{Tr}(R_0 + R_1^T)V$$

for all $n \in \mathbb{Z}_q$ and $V \in \mathcal{L}_p^0$, where $R_\mu = \mathrm{Tr}_2(|\mu\rangle\langle\mu| \otimes I_p)y^T_{j,n}$ for $\mu = 0, 1$ with the trace taken over the qubit. We note that both $R_{0,1} \geq 0$ are of rank-1 so that $R = R_0 + R_1^T \geq 0$ is at most of rank-2.

However, every nonzero $R \geq 0$ satisfying $\mathrm{Tr}(RV) = 0$ for all $V \in \mathcal{L}_p^0$ with $V \neq I$ is inevitably of rank 3 or more. In fact that is why we choose $\mathcal{L}_p^0$. To see this we denote $R_{ab} = \langle a|R|b\rangle$ and from $\mathrm{Tr}(RZ_p^a) = 0$ for all nonzero $a \in \mathbb{Z}_p$ it follows that $R_{aa} = r = \mathrm{Tr}R/p > 0$ is independent of a and from $\mathrm{Tr}(RX_pZ_p^a) = 0$ for $a \in \mathbb{Z}_p$ we obtain $R_{a,a+1} = 0$ for $a \in \mathbb{Z}_p$. If R were of a rank at most 2, then the determinants all 3×3 submatrices of R, especially those on the diagonal with entries labeled by $\{a, a+1, a+2\}$ and $\{a, a+2, a+3\}$, would vanish so that we would have $|R_{a+2,a}|^2 = r$ and $R_{a,a+3} = 0$, respectively, for $a \in \mathbb{Z}_p$. In the same manner, by induction, we would also have $|R_{a,a-2j}|^2 = r$ and $R_{a,a+2j+1} = 0$ for arbitrary $a, j \in \mathbb{Z}_p$ by considering the 3×3 submatrices labeled with $\{a, a+j, a+j+1\}$ and $\{a, a+j+1, a+j+2\}$. Since p is odd the equation $-2j = 2j+1$ has a solution $j_p = (p^2-1)/4$ in $\mathbb{Z}_p$ so that we would obtain $r = 0$, i.e., $R = 0$, a contradiction showing that every nonzero $R \geq 0$ satisfying condition ii is of rank 3 or more and thus $\mathrm{Tr}M_{U_0}(P_q \otimes H_{L_I}) > 0$.